UNIVERSITI PUTRA MALAYSIA

A NEW 128-BIT BLOCK CIPHER

FAKARIAH HANI BT HJ MOHD ALI

FSKTM 2009 5

A NEW 128-BIT BLOCK CIPHER

By

FAKARIAH HANI BT HJ MOHD ALI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in fulfilment of the Requirements for the Degree of Doctor of Philosophy

July 2009

Dedicated to my husband; Mohd Rafaie Abdul Razak,

my kids;Nurul Rusydina,Muhammad Fawwaz Hadi and Muhammad Faiz Hafizuddin,

my parents and family

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A NEW 128-BIT BLOCK CIPHER

By

FAKARIAH HANI HJ MOHD ALI

July 2009

Chairman : Associate Professor Ramlan Mahmod,PhD

Faculty : Science Computer and Information Technology

The evolvement of technology have resulted in a number of new proposals done on block ciphers such as KAMFEE, KAMKAR, ARIA, BLOWFISH256, DESL, REBC2, DSDP and etc. Even though there have been so much development of the block cipher, the industry still requires another block cipher as long as security features are met. Every country has different requirements when requesting block cipher so there is no limit in developing them. According to the National IT Council (NITC) report on "Securing Malaysia Sovereignty in the CyberWorld" provided by Ministry of Science, Technology and Innovation, Malaysia, they have outlined critical areas in which new and additional research and development is needed to increase the protection of the national information infrastructure. One of the critical areas is, secured communication which helps to protect the confidentiality and integrity of information during transmission and storage. Secured communication can be achieved by encrypting and hiding data transmission when it is stored on a system. One of the

areas which have been identified as priority with respect to secured communications is, conventional cryptography which provides the fundamental security and privacy in the information society. Towards that and after reviewing related research, in this research we propose to come up with a new 128-bit block cipher cryptographic algorithm which shall meet the security requirements.

This block cipher uses 128-bit for the key length and block size. It is an involution substitution and permutation encryption network (SPN). This block cipher uses only basic operations, key dependent S-box and XOR 's together so that it can be efficiently implemented on various platforms. The strength of this system is measured by NIST Statistical Test which evaluate from the point of view of the randomness of the block cipher output.

From the results, this new block cipher has successfully generated randomness of the block cipher output for data ranging from 1,000,000 to 6,000,000 bits. This means that the new block cipher is secured to be used for data ranging from 1,000,000 to 6,000,000 bits. This block cipher is suitable to be applied to small devices such as mobile phones and PDAs. The existence of this new 128-bit block cipher algorithm will increase the protection of the national information infrastructure and also will contribute as an alternative to other cryptographic algorithms in security in the computing industry.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

128-BIT BLOK CIPER BARU

Oleh

FAKARIAH HANI MOHD ALI

July 2009

Pengerusi : **Profesor Madya Ramlan Mahmod,PhD**

Fakulti : **Sains Komputer dan Teknologi Maklumat**

Perkembangan teknologi telah menyumbang kepada kewujudan banyak ciper blok yang baru seperti KAMFEE, KAMKAR, ARIA, BLOWFISH256, DESL,REBC2, DSDP dan lain-lain. Walaupun telah banyak pembangunan ciper blok ini, tetapi peringkat industri masih meminta ciper blok yang baru selagi ianya memenuhi ciri-ciri keselamatan. Setiap negara mempunyai berbeza-beza keperluan berkenaan blok ciper ini, jadi tidak ada had dalam pembangunannya. Berdasarkan kepada Perbadanan Teknologi Maklumat Kebangsaan yang melaporkan berkenaan "Securing Malaysia Sovereignty in the CyberWorld " yang telah dikeluarkan oleh Kementerian Sains, Teknologi dan Inovasi, Malaysia, mereka telah menggariskan beberapa perkara kritikal yang memerlukan tambahan penyelidikan dan pembangunan yang baru untuk meningkatkan perlindungan kepada infrastruktur maklumat kebangsaan. Salah satu bahagian yang dikenalpasti ialah keselamatan komunikasi yang mana ianya membantu melindungi rahsia dan integriti maklumat semasa proses penghantaran dan

menyimpan. Keselamatan komunikasi ini boleh dicapai melalui proses enripsi dan melindungi data ketika penghantaran dan penyimpanan dalam sistem. Salah satu bahagian yang telah dikenalpasti sebagai paling menyumbang kepada keselamatan komunikasi ialah kriptography konvensional yang mana menyediakan asas keselamatan dan privasi dalam bidang maklumat. Sehubungan dengan matlamat itu dan setelah mengkaji penyelidikan yang berkaitan, penyelidikan ini bercadang untuk membangunkan blok ciper 128-bit algoritma kriptografi yang memenuhi cirri-ciri keselamatan.

Ciper blok ini mempunyai saiz kunci 128-bit dan saiz blok 128-bit. Ianya hanya menggunakan operasi yang asas, mempunyai S-box yang dinamik dan XOR bersama dengan strukturnya supaya blok ciper ini boleh dilaksanakan dalam pelbagai platform. Kekuatan sistem ini diuji dengan menggunakan NIST Statistical Test yang mana kekuatan ciper blok ini akan diuji dari sudut kerawakan output ciper blok.

Berdasarkan kepada keputusan, ciper blok ini telah berjaya menjana output yang rawak untuk kadar data dari 1000000-6000000 bit. Ini bermakna ciper blok ini selamat untuk digunakan untuk kadar data dari 1000000-6000000 bit. Ciper blok ini boleh digunakan untuk perkakas yang kecil seperti telefon mudah alih dan PDA.

Kewujudan ciper blok ini akan mempertingkatkan lagi sistem keselamatan infrastruktur maklumat kebangsaan dan juga menyumbang sebagai alternatif kepada kriptografi algoritma dalam industri keselamatan komputer.

ACKNOWLEDGEMENT

Praise to Allah S.W.T. for giving me the strength, patience and motivation to complete this research.

My deepest appreciation and gratitude is dedicated to the research committee lead by Associate Professor Ramlan Mahmod, Associate Professor Ali Mamat, Associate Professor Azmi Jaafar and Mrs. Zaiton Muda for their motivation, guidance, encouragement, support and assistance throughout the research.

My deepest thank go to my husband, Mr. Mohd Rafaie Abdul Razak, parents, family , friends and colleagues at the Faculty of Computer Science and Information Technology, UPM, for their supports and encouragement during the process of completing this research.

As for financial support, I am grateful to University Technology Mara (UiTM) and Ministry of Higher Education for giving me scholarship while I was completing this research. Thank you all and may God bless all these individuals for their kindness.

I certify that a Thesis Examination Committee has met on 13 July 2009 to conduct the final examination of Fakariah Hani Bt Mohd Ali on her thesis entitled "A New 128-Bit Block Cipher" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Rahmita Wirza, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Abdul Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Abdul Azim Abdul Ghani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Abdul Hanan Abdullah, PhD
Professor
Faculty of Computer Science and Information Technology
University Teknologi Malaysia
(External Examiner)

BUJANG BIN KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 15 October 2009

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirements for the degree of Doctor of Philosophy. The members of the Supervisory Committee are as follows:

Ramlan Mahnod,PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Ali Mamat,PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Azmi Jaafar,PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Zaiton Muda,Msc
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

HASANAH MOHD GHAZALI,PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date : 16 November 2009

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

(FAKARIAH HANI BINTI MOHD ALI)

Date: July 2009

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.0 Introduction

Cryptography (or cryptology; derived from Greek '*kryptós* "hidden," and the verb '*gráfo'* "write" or *legein* "to speak") is the practice and study of hiding information. In modern times, cryptography is considered as a combination of mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depends on cryptography.

In modern times, cryptography is referred almost exclusively as encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (ie, ciphertext). Decryption is the reverse activity, which is, converting unintelligible ciphertext to plaintext. A cipher is a pair of algorithm which performs this encryption process and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (ideally, known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks. Symmetric-key cryptography is an encryption system in which the

sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. This contrasts with public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them.

Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES).

In 1997, the National Institute of Standards and Technology (NIST) US (an agency of the U.S Department of Commerce's Technology Administration) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities and to be adopted as Advanced Encryption Standard (AES). This new algorithm will replace Data Encryption Standard, which has been a standard since 1977. In 1998, NIST announced the acceptance of fifteen candidates of algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. NIST reviewed the results of this preliminary research and selected MARS, RC6™, Rijndael, Serpent and Twofish as finalists (Nechvatal et. al., 2000) (AES Development Effort, 2001). Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael (Daemen et. al., 1999) as the Advanced Encryption Standard (AES) (Nechvatal et. al., 2000) (AES Development Effort, 2001)(Burr, 2003). Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. According to Nechvatal et. al. (2000), Rijndael's combination of security,

performance, efficiency, implementability and flexibility makes it an appropriate selection for AES to use in the world of technology today and in the future.

There are many further analyses and improvements being done on Rijndael (Daemen et. al., 1999) (Federal Information Processing Standards Publication (FIPS) 197, 2001). McLoone et. al. (2001) proposed a Field Programmable Gate Arrays (FPGAs) Rijndael encryption design which utilizes look-up tables to implement the entire Rijndael Round function. Jing et. al. (2001) proposed a new algorithm for computing inverse in GF (2^m) on the standard basis. They proposed a set of multiplier and inverse in GF (2^m) to increase the computing speed. Sklavos et. al. (2002) proposed an alternative architecture and VLSI implementation design. These designs operate for both encryption and decryption process in the same device. Xinmiao et. al. (2002) addresses various approaches for efficient hardware implementation of the AES algorithm. Duong et. al. (2002) proposed the extended versions of AES to improve its strength and resistances against the rapidly increasing capability and strength of computers. Li (2004) proposed a parallel S-box architecture for AES byte substitution. AES S-box look-up table is separated into 32 small S-box look-up tables in order to parallel substitute the byte. Li (2005) presents an efficient s/s^{-1}-box look-up table based on content addressable memory (CAM) which can be used in both encryption and decryption of AES. The memory complexity is dramatically reduced compared to the SRAM based s-box and s^{-1}-box look-up tables. Zhang and Parhi (2006) presents 16 ways to construct the composite field $(((2^2)^2)^2)$ for the AES algorithm. Analytical results are provided for the effects of the irreducible polynomial coefficients on the complexity of each involving subfield operation. More development will be explained in chapter two.

1.1 Problem Statement

The evolvements of technology have resulted in a number of new proposals done on block ciphers. Murphy et. al. (2002 & 2003) proposed a new block cipher, BES, that uses only simple algebraic operation in GF(2^8). Elkamchouchi et. al. (2003) came up with new symmetric cryptosystem, the KAMFEE, which has a key dependent block length and key dependent rounds, enhanced by a rotor. The strength of this system as compared to the well-known DES, GOST, BLOWFISH, IDEA, RC5 and RIJNDAEL, gives excellent results looking from the point of view of security features and the statistics of the ciphertext. According to Daesung et. al. (2004), the authors propose a 128-bit block cipher ARIA which is an involution substitution and permutation encryption network (SPN). They use the same S-boxes as Rijndael to eliminate defects which are caused by a totally involution structure ARIA which uses only basic operations, S-box substitutions and XOR's together with an involution structure so that it can be implemented efficiently on various platforms. Mina et. al. (2004) presents a new block cipher KAMKAR 1.0. It uses a structure that resembles the famous cipher Rijndael. The difference between the two ciphers is that in the proposal the encryption process is made to be more key-dependent in order to have more strength against well-known attacks. Castro et. al. (2006) presents Wheedham: An Automatically Designed Block Cipher by means of Genetic Programming. Su et. al. (2007) proposed TWOFISH256. Twofish, proposed by Bruce Schneier et al., is a 128-bit block cipher that is constructed with Feistel Network. The cipher, one of the final candidates of AES, has a variable key length of 128, 192, and 256 bits. In this research, Twofish is expanded to a 256-bit block encryption algorithm.

Poschmann et. al. (2007) proposed a new block cipher, DESL (DES lightweight extension), which is strong, compact and efficient. Due to its low area constraints DESL is especially suited for RFID (radiofrequency identification) devices. Elkamchouchi and Elshafee (2007) present REBC2, Rotor Enhanced Block Cipher 2. RCBC2 is a new cryptosystem, developed on the concept of rotor enhanced block cipher which was proposed before by the authors in 2003. The rotor enhanced block cipher concept was considered from a new point of view, which is to use rotors to achieve two basic cryptographic operations; permutation, and substitution. According to Chen and Zhang (2008), the authors proposed a Key-dependent Cipher DSDP which uses both S-box and P-boxes that are all key-dependent.

Why do we need another block cipher? The industry still requires another block cipher as long as security features are met (Junod & Verdenay, 2004). As time goes by, the evolvement of technology will also contribute towards the development of new block ciphers. Every country has different requirements when requesting block cipher so there is no limit in developing them. According to the National IT Council (NITC) report on "Securing Malaysia Sovereignty in the CyberWorld" provided by Ministry of Science, Technology and Innovation, Malaysia (MOSTI, 2008), they have outlined critical areas in which new and additional research and development is needed to increase the protection of the national information infrastructure. One of the the critical areas is, secured communication which helps to protect the confidentiality and integrity of information during transmission and storage. Secured communication can be achieved by encrypting and hiding data transmission and also when it is stored on a system. One of the area which has been identified as priority with respect to secured communications is, conventional cryptography which provides the fundamental security and privacy in the information society. Towards that and after

reviewing related research, we propose to come up with a new symmetric cryptographic algorithm which shall meet the security requirements. This new block cipher will increase the protection of the national information infrastructure. The design of this new block cipher will consider all the security features in all the other block ciphers mentioned in the literature review.

1.2 Objective

The objective of this study is to design and implement new symmetric block cipher algorithm; which shall fulfill the security requirements.

Security is defined as to meet the requirements containing the properties of confusion and diffusion. In Shannon's original definition (Shannon, 1949), confusion refers to building a relationship between the key and the ciphertext until it becomes as complex and involved as possible. Diffusion is associated with non dependency of the bits of the ciphertext on the bits of the plaintext. Producing ciphers shall use the alternating substitution and transposition phases to achieve both confusion and diffusion respectively.

1.3 Scope of Research

The scope of this study is to develop new symmetric block cipher algorithm. For this new block cipher, the features which have been identified to be taken into consideration are:

a) Key length

The length of the Cipher Key is 128 bits.

b) Block Size

The length of the block size is 128 bits.

c) Round Function

The component in round function consists of Key Scheduling (), AddSubKey() , ShiftCol() , ChangeByte() and SwapPost() processes

d) Confusion and Diffusion/ Randomness test

The evaluation criteria will be based on the NIST Statistical Test Suite (Rukhin et. al, 1997). NIST used this test suite in selecting the Advanced Encryption Standard (Soto, 1999) (Soto & Bassham, 2000). The aspect of security which will be focused in this research is the randomness of the block cipher output.

1.4 Organization of the Thesis

This thesis is organized in such a way so that the reader can get a clear view of the objectives of the study. The current chapter introduces the problem and the research objectives to be attained and also the research scopes. This is the main starting point of the purpose for the study.

Chapter 2 describes literature surveys and background study on some related works. It covers the background of cryptography, how cryptography works, and also

comparison between conventional and public key cryptography. This chapter also includes detailed description on the most common algorithm used for secret key and public key systems.

The third chapter describes the research methodology. This chapter describes how the researcher conducts this research. This chapter also explains all the experimental design that will used to select the number of rounds and the process of measuring confusion/diffusion or randomness of the block cipher output.

The fourth chapter discusses on system design adapted by the study. This chapter also specifies the new block cipher algorithm in detailed. It will cover the definitions, notations and conventions, mathematical preliminaries and algorithm specifications. It also contains validation of methods used. The fifth chapter covers coding and implementation of the algorithm. It is an important stage where the defined procedures are transformed into control specifications with the help of a computer language. Before actually implementing the new system into operation, a test run of the system is done by removing bugs, if any. It is an important phase of a successful system.

The sixth chapter will discuss the results and the findings of the new block cipher algorithm. Finally, the seventh chapter is the conclusion of the study and suggestion for further efforts which can be done to accomplish the study.